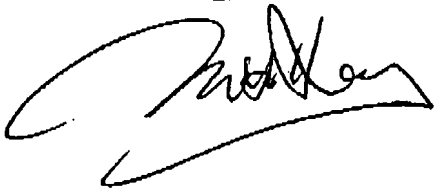
Please change the title to be read as "Computer Apparatus/Software Access Right Management".

Respectfully submitted,

Ho Keung, Tse.



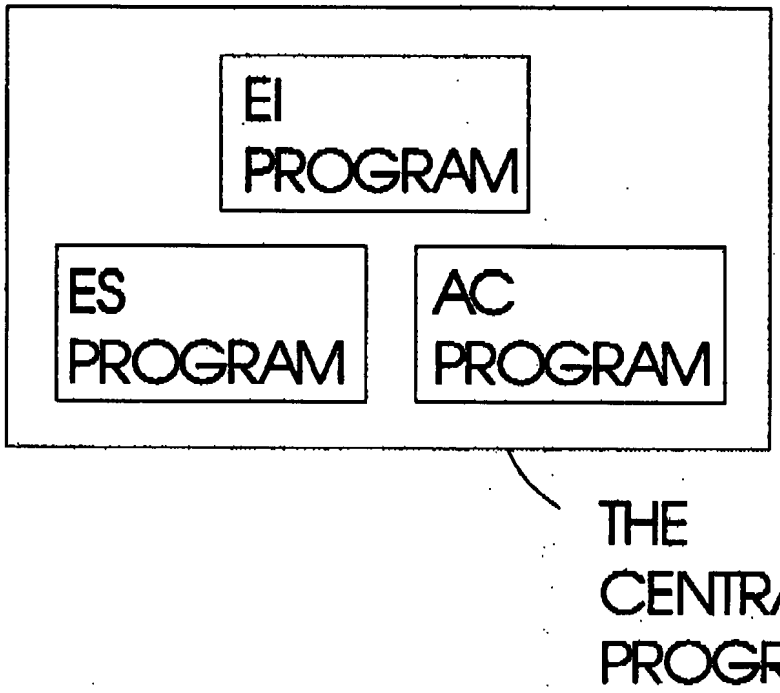
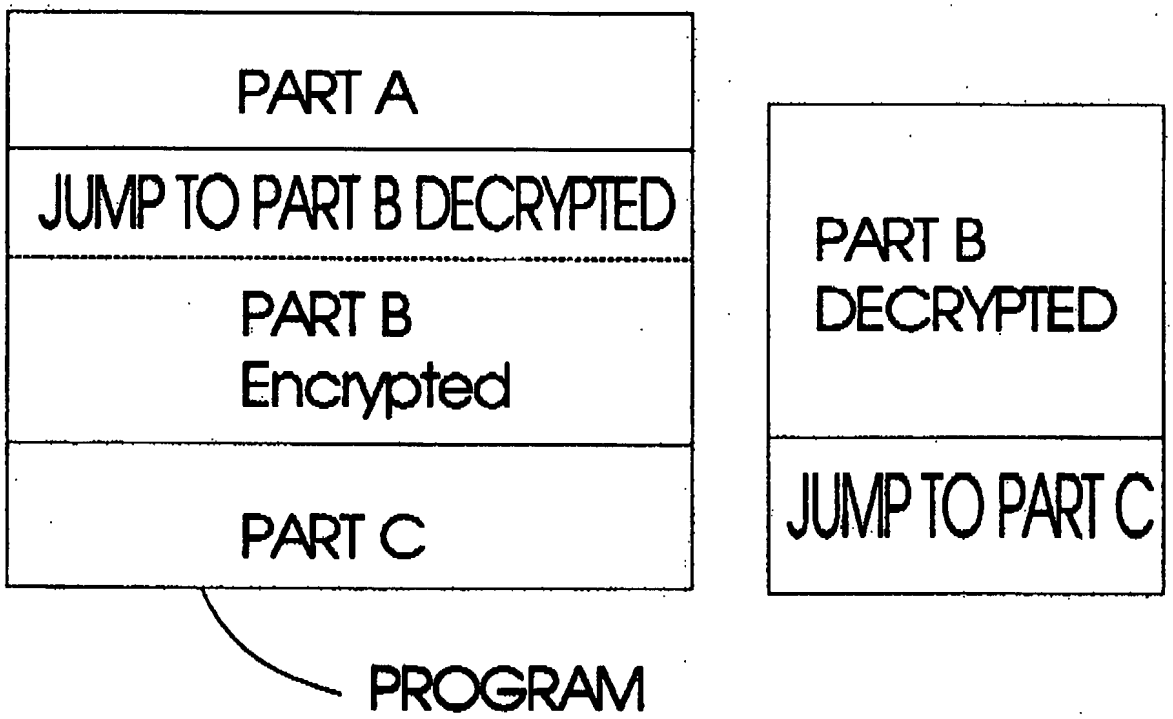


FIG. 1

FIG. 2



COMMENT

20 claims presented. Claims 1, 7, 10, 12 , 14, 16-18, 20 are independent.

Claims 2, 4-6 depends directly or indirectly on independent claim 1.

Claims 8, 9 depend directly on independent claim 7.

Claim 11 depends directly on independent claim 10.

Claims 3, 13, 19 depend directly on independent claim 12.

Claim 15 depends directly on independent claim 14.

Claims 1-18 amended. New claims 19, 20 submitted.

Independent claims 1, 7, 10, 12, 14, 16, 17, 18 require existence of identity means or information or program code or system "capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of the software desired to be protected has to be responsible", to obtain a "discouraging effect" for discouraging a user from enabling other user to use the software desired to be protected.

It should be noted that, independent claims 1, 7, 10, 12, 14, 16, 17, 18 recites that "without causing a electronic commerce operation being performed", thus **precluding all prior art in related to receiving user payment for use of software.**

Independent claims 7 recites the "authorising program code for providing user access to the software desired to be protected", is being effectively under the control of the user thereof, this implies that the rightful user(s) can use the authorising program code to access the protected software without any restriction such as payment.

The present invention as defined by claim 7 allow unrestricted rightful use of protected software while offering protection against unauthorised use by requiring the authorising software be contained in the protection software with the identity software, and can not be copied therefrom individually.

Claim 10 corresponding to the third embodiment as readable on original description, sheet 10, second and third paragraphs.

Independent claims 16, 17, 18 , recite recites a step (b), (c), (a) respectively, for **recognising a processing device**, in the present of an identity information or system and **thereafter, permitting use of software desired to be protected thereon**. This is another innovative feature of the present invention not being suggested or disclosed by the cited prior art reference, either considered individually or in combination.

Particularly, Claim 16 recites "obtaining from a user first information" and it has to be consistent with third information necessary for enabling electronic transaction(s) for which a rightful user of the software desired to be protected has to be responsible; and the method is being performed without causing a said transaction take place .

Claim 17, in particular, recites verifying an account of a user being valid, to obtain the "discouraging effect". Claim 17 further recites a sub-method recognises a processing device, for a cost from that user . It is clearly understood that the cost is for the use of the protected software on that recognised processing device by that user, because thereafter no further charge therefor, as readable on step (e).

Independent claims 17 further recites, the sub-method can be used for recognising another processing device, without re-charging the cost.

Thus, a user who has paid for the protected software, can use the same on any processing device he desires or on the original processing device even after changes in software/hardware, without being fully re-charged, by using a discouraging effect to assure the software vendor that the protected software will continue to be used by that user.

Claim 18 recites "the presence of identity information/system in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform ... step (a)". This actually means that the protection software either determines the presence of identity information/system, like claim 1, or being combined with the identity program code in a non-separable manner, like claim 7.

Comment on Yuval et al.

As Yuval et al. was published on Dec 17, 1996, after the priority date Dec 1, 1995 of the present application, therefore **any rejection so raised should be 35 U.S.C. 102(e).**

As readable on claim 1, the patent is directed to a method for controlling unauthorised access to information distributed to users, comprising the steps of:

.....;

encrypting the information;

receiving identifying information(ID) from a user;

generating a numeric representation(X) of the ID ;

generating a unique user key(Y) using X and decryption key of the encrypted information ;

providing the user with the unique user key ; and decrypting the encrypted information using X, Y.

Other claims such as claim 21 recites 2 numeric representations and 2 unique user keys etc, but principle behind them and claim 1 are the same.

And, as readable on col. 7 last paragraph-col. 8 first paragraph, ID can be determinable from XY & X, so as to trace the user who reveals them to an unauthorised user.

Further, Yuval et al also suggest, "To provide a higher level of security, the identifying information should include information that the user would not want to divulge to others (e.g., a credit card number...)".

Thus, Yuval et al's patented invention is similar with the present application in that it discloses protecting software, by requiring the present of user identity information as a precondition for accessing software .

Although not explicitly indicated in Yuval et al's document, once a user enters his ID and user key Y into a computer, they will automatically converted into be

information in a machine-readable only form storing at a location unknown to any user.

In other words, even if the ID including credit card information, it is **not capable of being used in enabling electronic commerce operation(s)** and this is required by my independent claims.

Further, it would not be possibly expected that it could provide the "discouraging effect" as suggested by the present application. Unless an inventive step is being made for converting the machine-readable only form information storing at the unknown location into to a user accessible form, such as causing a display thereof.

And, without expecting the "discouraging effect", it would further impossible for one with ordinary skill in the art to **permanently** storing the machine readable only form information in that unknown location, rather than the decryption key or the product XY obtained there from, for eliminating the hassle of repeatedly entry of ID and user key by user. As the latters can be used more directly for decrypting the encrypted information, and as mentioned above, Yuval et al disclose that XY can also be used to trace the user.

Argument for overcoming Haas et al.

Haas et al. was patented on Feb. 17, 1998, whereas the present application has a priority date of Dec1, 1995. Therefore, **any rejection raised basing thereon should be 35 U.S.C. 102(e)**, and only the patented invention should be included into prior art, excluding the description.

Even though it is readable **on the description**, column 5, lines 47-54, Haas et al. teach a deterrent as causing by a software, a rightful user's credit card number to be displayed, to discourage a rightful user from sharing the software which being for decrypting a commercial software product, to other people. **This is not readable on the claims.**

In Haas et al.'s claims 14, 16, there do describe a method intended to discourage a predetermined user from sharing an encryption key with another user, by obtaining a credit card number from the predetermined user and then communicating the credit card number to the predetermined user during a step of decrypting. This has no support from the description and it is unclear in what way the credit card number is communicated to the predetermined user and why by doing so, this can discourage the predetermined user from sharing an encryption key with another user. The 2 claims are nonsense and undefined.

Accordingly, the Examiner is respectfully requested to withdraw the two 35 USC 103 (a) rejections relying on Haas et al.

-1(Dirty Version)-

Computer Apparatus/Software Access Right Management

This is a continuation-in-part of patent application serial no. :08/587,448, filed on 12/01/95, which is still pending.

Field of the invention

The present invention relates to protection of software/data processing apparatus, and particularly, to protection of [software] them against unauthorised/illegitimate use [or copying].

Background of the invention

Conventionally, [software protection] methods for protecting commercial software products such as programs, multimedia software, distributed through a communication network, such as a telephone system, require a user computer to have a piece of hardware comprising decryption keys and system be installed therein, for to be authenticated by a software program running on the computer. Hardware, rather than software, are being used because software duplication facilities are commonly found in personal computers. However, this is extremely cumbersome and places a large burden on users and vendors alike.

It is therefore an object of the present invention to provide a piece of software to replace the above-mentioned piece of hardware and the rightful user of that piece of software is being discouraged from copying it to someone else[, by means of a psychological barrier].

It is therefore another object of the present invention [is] to provide a method to discourage a rightful user from copying his software to someone else .

It is therefore a further object of the present invention to provide a method to verify the identity of a user of data processing apparatus .

Summary of the invention

According to a first embodiment of the present invention, there is provided a central program comprising 1) a sub-program for providing an Encrypted Identity (herein below referred to as EI sub-program), 2) a sub-program for authorising use of a software [product](herein below referred to as AS sub-program), 3)a sub-program for authenticating user computer (herein below referred to as AC sub-program).

The central program is for managing the use of the individual sub-programs therein so that the AS sub-program can be protected from being accessed directly, thereby preventing it from being copied individually. The EI sub-program is for providing identity information(an encrypted identity) of its rightful owner for accessing a network central computer to obtain services or software products or alike in which a secure operation on a user account of that owner for payment therefor involved. The AC sub-program is for authenticating the computer on which it runs as being a particular predetermined computer, by determining the hardware and software configuration as well as hardware characteristics of that computer by software means and comparing the result with that required. The AS sub-program is for using the authentication result of the AC sub-program and the existence of the EI sub-program which being not protected against unauthorised use and being capable of being used by any user thereof, on a computer, as preconditions for authorising those software [products] which may be purchased commercial computer software obtained to be used on that computer.

It should be noted that in the central program, as far as protection of the software products from being unlawfully copied by the rightful user to someone else is concerned, the AS sub-program is the only sub-program which needs protection and according to the present invention, the AS sub-program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a rightful user would not copy a software, i.e., the central program in which the EI sub-program exists and which can be used by an unauthorised user to provide the rightful user's

identity information for using the rightful user's account in obtaining, for e.g., network services or software products, to someone else. As seen from the use of automatic teller machine(ATM) magnetic cards, which although can readily be forged, has been proved to be remarkably secure.

According to a second embodiment of the present invention, the central program comprising the EI sub-program only, and the AS sub-program become an individual program which authorises the software product(s) to be used only when the EI sub-program exists in the same computer it runs and which is being determined by receiving an encrypted identity of the EI sub-program from the same.

According to a third embodiment, the EI and AS sub-programs are basically equivalent such that copying the AS sub-program by its rightful user to someone else is equivalent to copying the EI sub-program to someone else, thereby preventing the AS sub-program from unauthorised copying or use.

Brief description of drawings

FIG.1 is a block diagram of the central program.

FIG.2 is a diagrammatic view of a program in which a part B thereof being encrypted, in RAM space.

Detailed description of the preferred embodiments

One object of the [The] present invention is [directed] to [protecting] protect software product(s) distributed through a communication network, against unauthorised copying or use, and for the sake of simplicity, the following description is directed to protection of such software product(s) stored in a user's IBM PC computer. And, the first embodiment of the present invention will be described under the following headings:

1) The Central Program.

2) The Sub-program for providing an Encrypted Identity (EI sub-program).

3) The Sub-program for authorising use of a software product (AS sub-program).

-13(Claim Dirty Version)-

What is claimed is :

1.(Third time Amended) A method for protecting software from unauthorised use , comprising the steps of :

determining if identity system/information, is existing in a processing apparatus ;

[determining the existence of an identity means in association with a computing means ;]

using a favourable result of said determination as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

[using a favourable result of said determination of existence as a pre-condition for permitting use of said software desired to be protected on said processing means ;]

wherein :

said identity system/information, if so existing, being capable of being used in enabling electronic commerce operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

[wherein said identity means being for enabling electronic money transfer operation(s) for which a rightful user of said software desired to be protected has to be responsible ;]

access to said software desired to be protected is being provided without causing a said operation being performed and said identity system or information being specific to said rightful user and said software desired to be protected being licensed to said rightful user.

[wherein said rightful user being a user who has already obtained a right of using said software desired to be protected, with any necessary payment therefor, being made ; and the use of said software desired to be protected is being permitted without a said operation being performed .]

2. (Second time Amended) A method for protecting software from unauthorised use, as claimed in claim 1 , wherein further comprising the steps of :

authenticating said identity [software] system/information ;

determining said identity [software] system/information [will be determined] as existing [in said memory means], if the result of said authentication is favourable and as not existing if otherwise .

3. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information, and for providing user access to third software if said authentication result is favourable .

4. (Second time Amended) A method for protecting software from unauthorised use , as claimed in claim 1 , wherein said operation being operation related to making payment from an account of said rightful user.

5. (Second time Amended) A method for protecting software from unauthorised use , as claimed in claim 1 , wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

6. (Second time Amended) A method for protecting software from unauthorised use , as claimed in claim 5 , wherein further comprising the steps of:

storing an encrypted identity of [its rightful] a user in said processing apparatus ;

if [one] all of said protected programs stored in said [computer] processing apparatus has a valid user identity which being [not] consistent with the decryption result of said stored encrypted identity [in said authorising software], [said authorising software will not permit] permitting use of said protected programs .

-16(Claim Dirty Version)-

7. (Third time Amended) A computer software product for protecting software publicly distributed against unauthorised use ;

[Protection software for use on a computing device, to protect software against unauthorised use ;]

said software product comprising :

[said protection software comprising :]

identity program code for enabling electronic commerce [identity software being essentially used on said computing device in enabling] operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

authorising [software] program code effectively under the control of said rightful user for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed [permitting use of said software desired to be protected, on said computing device] ;

a computer readable medium storing said identity program code and said authorising program code ;

Wherein :

said identity [software] program code and said authorising [software] program code are contained in said [protection] software product in such a manner that said authorising [software] program code is prevented from being copied therefrom individually; and

the improvement resides in said protection basing on no hardware and/or software specific to said rightful user other than said identity program code and said identity program code being specific to said rightful user .

8. (Second time Amended) A computer software product for protecting software [Protection software] as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful user.

9. (Second time Amended) A computer software product for protecting software [Protection software] as claimed in claim 7, wherein [said authorising software contains said identity software] said computer readable medium being in the form of data signal embodied in a carrier wave.

10. (Third time Amended) A computer software product for protecting other software against unauthorised use , comprising :

[Authorising program for use on a computing device, to protect other software against unauthorised use ;]

a program for, when being executed on a processing apparatus, providing user access to said software desired to be protected ;

[said authorising program being effectively under the control of a rightful user of said software desired to be protected for, when executed, permitting use of said software desired to be protected on said computing device ;]

a computer readable medium storing said program ;

wherein :

information [related] specific to [said] a rightful user of said software desired to be protected, exists in said [authorising] program as a part thereof and being accessible to the user thereof ;

[said information being essentially used on said computing device in enabling operation(s) for which said rightful user has to be responsible]

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user has to be responsible, but not being usable by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said processing apparatus as a part thereof, and access to said software desired to be protected is being provided without causing a said operation being performed .

11. (Second time Amended) [Authorising program] A computer software product as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user.

12. (Third time Amended) A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a [computing device] processing apparatus having [storing] an identity [software] program code/means ;

using said first information received being correct as a pre-condition for [permitting use of said software desired to be protected on said computing device] causing said processing apparatus to provide user access to said software desired to be protected ;

wherein :

said identity [software] program code/means being for providing a second information [related] specific to [the] a rightful user of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

[and] said second information being [essentially] capable of being used in enabling electronic [money transfer] commerce operation(s) for which said rightful user has to be responsible ;

[wherein said rightful user being a user who has already obtained a right of using said software desired to be protected, with any necessary payment therefor, being made ; and the use of said software desired to be protected is being permitted without a said operation being performed]

access to said software desired to be protected is being provided without causing a said operation being performed.

13. (Second time Amended) A method for protecting software from unauthorised use, [Authorising program] as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user and said first information being a password.

-20(Claim Dirty Version)-

14. (Third time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[authenticating identity information existing in a memory means associated with said computing means ;]

authenticating identity information/system associated with a processing apparatus ;

using a favourable result of said authentication as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected [permitting use of said software desired to be protected on said computing means] ;

wherein said identity information [being essentially used on said computing means in enabling electronic money transfer] /system existing in such a manner that said identity information/system being capable of being used in enabling electronic commerce operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

[wherein said rightful user being a user who has already obtained a right of using said software desired to be protected, with any necessary payment therefor, being made ; and the use of said software desired to be protected is being permitted without a said operation being performed.]

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/system being specific to said rightful user and said software desired to be protected being licensed to said rightful user.

15. (Second time Amended) A method for protecting software from unauthorised use , [Authorising program] as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user.

16. (Second time Amended) A method for protecting software [distributed by a vendor] from unauthorised use , comprising the steps of :

[obtaining by an installing software running on a computing device , first information from a user ;]

(a) obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;

[determining, by said installing software, from said computing device second information related to the hardware or/and software thereof , if said first information received being confidential information of a rightful user of said software desired to be protected ;]

(b) determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software ; thereafter

[thereafter, determining by said installing software, from the computing device onwhich said installing software runs, third information related to the hardware or/and software thereof;]

[determining , by said installing software, if said third information is consistent with said second information ;]

(c) authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;

[using, by said installing software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the computing device onwhich said installing software runs ;]

(d) using a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

[Wherein said installing software being supplied from said vendor to said rightful user.]

wherein said third information being confidential information of a rightful user of said software desired to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible ; and said method is being performed without causing a said transaction take place .

-23(Claim Dirty Version)-

17. (First time Amended) A method for protecting software from unauthorised use, by restricting the use thereof to be under control of a single person, comprising a sub-method ; said sub-method comprising the steps of :

[a) determining, the existence of an identity software/means which being essential used in a computing device, say first computing device, for accessing a remote electronic transaction system an account of a rightful user of said software desired to be protected, in said computing device, by an installing software ;]

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

[b) establishing a communication between said computing device and a computing means of said remote electronic transaction system, for verifying said account is a valid account ;]

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being communicated to said remote electronic transaction system from said processing apparatus ;

[c) using by said installing software running on said computing device, a favourable result of said determination of existence and verification as pre-conditions for determining from said computing device first information related to the hardware or/and software thereof ;]

(c) using a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

[thereafter, determining by said installing software, from the computing device onwhich said installing software runs, say second computing device, second information related to the hardware or/and software thereof;]

[determining , by said installing software, if said first information is consistent with said second information ;]

(d) authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

[if the result of said determination of consistence is not favourable, repeat step a) to c) with said second computing device ; otherwise, using by said installing software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on said second computing device ;]

(e) using a favourable result of said authentication as a pre-condition for permitting use of said software on said second processing apparatus, with no charge ;

[wherein said rightful user being a user who has already obtained a right of using said software desired to be protected on any suitable computing devices, with any necessary payment therefor, being made ; and said installing software being specific to said rightful user .]

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

18.(First Time Amended) A method for protecting software [distributed by a vendor] from unauthorised use, comprising [the steps of] a sub-method ;

[using, an installing software running on a computing device, "the existence of an identity software/means which being essentially used in said computing device for enabling electronic money transfer operation(s) for which a rightful user of said software desired to be protected has to be responsible, in said computing device" ; as a pre-condition for determining from said computing device first information related to the hardware or/and software thereof , without causing a said operation being performed ;]

wherein said sub-method a protection software being used and "the presence of identity information/system in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information/system being specific to a user and capable of

being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a) determining by said protection software running on a processing apparatus, say, first processing apparatus with said precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

[thereafter, determining by said installing software, from the computing device onwhich said installing software runs, second information related to the hardware or/and software thereof;]

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof ;

[determining , by said installing software, if said first information is consistent with said second information ;]

(c) determining if said second information is consistent with said first information ;

[using by said installing software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the computing device onwhich said installing software runs; without causing a said operation being performed .]

(d) using a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

19. A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

20. A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

using by said data processing apparatus, a favourable result of said verification as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said account not being charged and said at least a part of functionality being not related to said validity status of said account.

-13(Clean Version)-

What is claimed is :

1. A method for protecting software from unauthorised use , comprising the steps of :

determining if identity system/information, is existing in a processing apparatus ;

using a favourable result of said determination as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein :

said identity system/information, if so existing, being capable of being used in enabling electronic commerce operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed and said identity system/~~or~~ information being specific to said rightful user and said software desired to be protected being licensed to said rightful user.

2. A method for protecting software from unauthorised use, as claimed in claim 1 , wherein further comprising the steps of :

authenticating said identity system/information ;

determining said identity system/information as existing, if the result of said authentication is favourable and as not existing if otherwise .

3. A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information, and for providing user access to third software if said authentication result is favourable .

4. A method for protecting software from unauthorised use , as claimed in claim 1 , wherein said operation being operation related to making payment from an account of said rightful user.

5. A method for protecting software from unauthorised use , as claimed in claim 1 , wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity

information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

6. A method for protecting software from unauthorised use , as claimed in claim 5 , wherein further comprising the steps of:

storing an encrypted identity of a user in said processing apparatus ;

if all of said protected programs stored in said processing apparatus has a valid user identity which being consistent with the decryption result of said stored encrypted identity, permitting use of said protected programs .

7. A computer software product for protecting software publicly distributed against unauthorised use ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

authorising program code effectively under the control of said rightful user for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed ;

a computer readable medium storing said identity program code and said authorising program code ;

Wherein :

said identity program code and said authorising program code are contained in said software product in such a manner that said authorising program code is prevented from being copied therefrom individually; and

the improvement resides in said protection basing on no hardware and/or software specific to said rightful user other than said identity program code and said identity program code being specific to said rightful user .

8. A computer software product for protecting software as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful user.

9. A computer software product for protecting software as claimed in claim 7, wherein said computer readable medium being in the form of data signal embodied in a carrier wave.

10. A computer software product for protecting other software against unauthorised use , comprising :

a program for, when being executed on a processing apparatus, providing user access to said software desired to be protected ;

a computer readable medium storing said program ;

wherein :

information specific to a rightful user of said software desired to be protected, exists in said program as a part thereof and being accessible to the user thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user has to be responsible, but access to said software desired to be protected is being provided without causing a said operation being performed .

11. A computer software product as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user.

12. A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity program code/means ;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein :

said identity program code/means being for providing a second information specific to a rightful user of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

said second information being capable of being used in enabling electronic commerce operation(s) for which said rightful user has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed.

13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user and said first information being a password.

14. A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/system associated with a processing apparatus ;

using a favourable result of said authentication as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein said identity information/system existing in such a manner that said identity information/system being capable of being used in enabling

electronic commerce operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/system being specific to said rightful user and said software desired to be protected being licensed to said rightful user.

15. A method for protecting software from unauthorised use, as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user.

16. A method for protecting software from unauthorised use , comprising the steps of :

(a) obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;

(b) determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software ; thereafter

(c) authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;

(d) using a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

wherein said third information being confidential information of a rightful user of said software desired to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible ; and said method is being performed without causing a said transaction take place .

17. A method for protecting software from unauthorised use, by restricting the use thereof to be under control of a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being communicated to said remote electronic transaction system from said processing apparatus ;

(c) using a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

(d) authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

(e) using a favourable result of said authentication as a pre-condition for permitting use of said software on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

18. A method for protecting software from unauthorised use, comprising a sub-method ;

wherein said sub-method a protection software being used and "the presence of identity information/system in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information/system being specific to a user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a) determining by said protection software running on a processing apparatus, say, first processing apparatus with said precondition being met,

first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof ;

(c) determining if said second information is consistent with said first information ;

(d) using a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

19. A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

20. A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

using by said data processing apparatus, a favourable result of said verification as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said account not being charged and said at least a part of functionality being not related to said validity status of said account.